Integritas Suricata *Intrusion Detection System* (IDS) dengan Mikrotik *Firewall* untuk Keamanan Jaringan Fakultas Teknologi Informasi Universitas Kristen Satya Wacana

[1]Oktriany Susanti Sundun , [2]Teguh Indra Bayu
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50715, Indonesia
Email: [1)]672014172@student.uksw.edu, [2)]teguh.bayu@staff.uksw.edu

Abstract

This research look at the integrity of suricata with mikrotik to detect port-based attacks and protocol. The application used to design the system is suricata. Suricata is one of a software other than a snort that is capable for working as an IDS, IPS and monitoring. Suricata will work as a third party that helps the performance of firewall mikrotik also required a barnyard that will read the output file of the suricata which tend to be a binary and send the log files into the database.

Suricata works based on a signature-base, where each packet is checked on the basis of the existing rules on suricata. Suricata will produce a binary output called unified. alert. Barnyard will be tasked for translating the output file and also sending it to the database, and then mikrotik will take a file from the database to be followed up. Besides, this research design requires an application of firewall Demilitarized Zone (DMZ) it is done to protect network LAN from an attack.

Abstrak

Penelitian ini melihat integritas antara suricata dengan mikrotik untuk mendeteksi serangan yang berbasis port dan protokol. Aplikasi yang dipakai untuk mendesain sistem ini adalah suricata. Suricata merupakan salah satu *software* selain snort yang mampu bekerja sebagai IDS, IPS dan *monitoring*. Suricata akan bekerja sebagai pihak ketiga yang membantu kinerja dari *firewall* mikrotik selain itu dibutuhkan juga barnyard yang akan membaca file output dari suricata yang bersifat binari dan mengirimkan *log* file tersebut ke dalam database.

Suricata bekerja berdasarkan *signature-base*, setiap packet akan diperiksa berdasarkan *rules* yang ada pada suricata. Suricata akan mengeluarkan sebuah *output* binari yang disebut *unified.alert*. Barnyard akan bertugas menerjemahkan file *output* dan juga mengirimkan ke database, lalu mikrotik akan mengambil file dari database tersebut untuk ditindak lanjuti. Selain itu, desain pada penelitian ini membutuhkan penerapan *firewall Demilitarized Zone* (DMZ) hal ini dilakukan untuk melindungi jaringan LAN dari suatu serangan.

Kata Kunci:
Suricata, Barnyard, Mikrotik

[1)]Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.
[2)]Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.